UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/762,680 | 01/21/2004 | Osamu Kobayashi | GENSP047 | 5247 |

22434 7590 06/26/2007

BEYER WEAVER LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

| EXAMINER | |
|---|---|
| SHAIFER HARRIMAN, DANT B | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/26/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/762,680 | KOBAYASHI, OSAMU | |
| | Examiner | Art Unit | |
| | Dant B. Shaifer - Harriman | 2109 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *4/16/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/2/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Objections*

1. Claim 15 is objected to because of the following informalities: Grammar correction: the limitation "an particular control value," should be "a particular control value". Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim 20 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 20 recites the limitation "signals" in second line of claim 20. There is insufficient antecedent basis for this limitation in the claim. "Signals," will be treated as the equivalent of the "values" of claim 3.

Claim 15 is rejected under 35 U.S.C. 112, second paragraph, as being vague and indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear how a "a particular control value CNTL3" differs from a "a control value CNTL3."

## *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim(s) 1, 6, 7, 12, 17, 18 are rejected under 35 U.S.C. 102(b) as being taught by Huuhtanen (Publication # EP 0 674 441 A1)

***Huuhtanen teaches:***

Claim #1. A packet based high bandwidth copy protection method comprising:

- forming a number of data packets at a source device (Col. 3, lines 35 – 41 & Col. 3, lines 47 – 50, the examiner notes that the source device is the TV operators equipment, the operators signal to the digital cable box that the customer receives is both scrambled (encrypted) and unscrambled signals or data packets that is for TV programming service operation.);

- forming a first group of encrypted data packets by encrypting some of the data packets based upon a first set of encryption/decryption values, wherein the number of encrypted data packets in the first group of encrypted data packets is less than the number of data packets formed at the source device;( Col. 3, lines 47 – 50, the examiner notes that by sending both scrambled and unscrambled data packets to the customer, this means that a selected or specific group of packets from the many packets that were formed at the source device was chosen for encryption, this will show that the number of scrambled

data packets chosen form a large group will be smaller than the overall number of data packets that were formed at the source device.)

- transmitting the encrypted and unencrypted data packets from the source device to a sink device coupled thereto(Col. 3, lines 47 – 50);

- decrypting the first group of encrypted data packets using the first set of encryption/decryption values(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink device.); and

- accessing the decrypted and unencrypted data packets by the sink device(Col 3, lines 5 – 10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit.)

Claim #6. A system for providing high bandwidth copy protection in a packet based system, comprising:

- a source unit arranged to provide a number of data packets (Col. 3, lines 35 – 41 & Col. 3, lines 47 – 50, the examiner notes that the source device is the TV operators equipment, the operators signal to the digital cable box that the customer receives is both scrambled (encrypted) and unscrambled signals or data packets that is for TV programming service operation.);

- a sink unit coupled to the source unit arranged to receive the data packets from the source unit(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit.);

- an encryption unit coupled to the source unit arranged to encrypt selected ones of the data packets sent from the source unit to the sink unit(Col 3, lines 5 –10 & Col. 3, lines 47 – 50, the examiner notes that the cable service operator encrypts the signal before the signal is transmitted to the customers receiver, which conveys that there is a encrypting device attached to the source or transmitter or the cable TV operators equipment, furthermore the customer has a descrambling device attached the signal receiver for the decryption of the signals or data packets that are incoming to the customers receiver.);

- a decryption unit coupled to the sink unit arranged to decrypt the encrypted data packets(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit.);

- an encryption/decryption values generator arranged to provide a set of encryption/decryption values to the decryption unit that, in turn, uses the decryption values to-decrypt any appropriately encrypted data packets; and processing the decrypted and unencrypted data packets by the sink unit (Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit that will

posses the necessary decryption values generator that will arrange for the decrypting of the selected encrypted data packets received by the sink device.)

Claim #7. A system as recited in claim 6, wherein:

wherein

- the source unit is a video source(Col 3, lines 5 –10, the examiner notes that the source device is the TV operators equipment)

and wherein

- the sink device is a video display (Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink device, the receiver will undoubtedly be a set a top box attached to a television, due to the fact the operators service is a signal for paid subscribes to watch cable television.)

and wherein:

- the number of data packets include some audio data packets and some video data packets (Col. 3, lines 35-41 & Col 3, lines 5 –10, the examiner notes that the service operator has the transmitter or source device, and the customer has the set up top box, which is a receiver or sink device, the examiner further notes that "picture and sound quality," are a strong indication that the data packets consists of both video and sound content or data packets.)

Claim #12. Computer program product executable by a processor for providing a packet based

high bandwidth copy protection, the computer program product comprising:

- computer code for forming a number of data packets at a source device (Col. 3, lines 5 – 9 & Col. 3, lines 47 – 50, the examiner notes that the customers receiver (i.e. cable box) can be considered a computer program product. Based on the fact that a cable box has both a hardware and software components, without hardware or software component, the other component will be unable to operate; the cable box contains the necessary software to request and retrieve TV programming (i.e. movies, sporting events etc.) from the operators server (forming a number of data packets at the operators server.), moreover the operators receiver or cable box contains the software necessary to implement the goods and services promised by the operator, which is through the execution of the operators server, which contains the operators multimedia, processor.)

- computer code for encrypting some of the data packets based upon a set of encryption values (Col. 3, lines 5 – 9 & Col. 3, lines 47 – 50, the examiner notes that the customers receiver (i.e. cable box) can be considered a computer program product. Based on the fact that a cable box has both a hardware and software components, without hardware or software component, the other will be unable to operate; the cable box contains the necessary software to request and retrieve TV programming (i.e. movies, sporting events etc.) from the operators server (forming a number of data packets at the operators server.), moreover the operator receiver or cable box contains the software necessary to implement the goods and services promised by the operator, which is through the execution of the operators server (which contains the operators multimedia content

processor.) The customers receiver will also have the necessary software for encryption/decryption generator for sending encrypted messages (i.e. cable box malfunction indications that facilitates problem solving and better customer service, for example sending multimedia data packets back to the operators server (i.e. if there is a an error in the sending of multimedia content, the receiver will request that a particular data packet be sent back to the receiver in order to complete the multimedia content transmission to the customer and will be encrypted so that a hacker cannot gain information on how to break into a the cable TV system.)

wherein:

- the number of encrypted data packets is less than the number of data packets formed at the source device(Col. 3, lines 47 –50, the examiner notes that many data packets are formed at the operators source device and only a selected few of that many data packets at the source are chosen to be encrypted.);

- computer code for transmitting the encrypted data packets and the unencrypted_data packets from the source device to a sink device coupled thereto(Col. 3, lines 5 – 9, the examiner notes that the customers receiver(i.e. cable box) can be considered a computer program product. Based on the fact that a cable box has both a hardware and software components, without hardware or software component, the other will be unable to operate; the cable box contains the necessary software to request and retrieve (i.e. transmitting/receiving) TV programming (i.e. movies, sporting events etc.) from the operators server (forming a number of data packets at the operators server.), moreover the

operators receiver or cable box contains the software necessary to implement the goods and services promised by the operator, which is through the execution of the operators server ( which contains the operators multimedia processor.);

- computer code for decrypting the encrypted data packets based in part upon the encryption values (Col. 3, lines 5-9, the examiner notes that the cable box or the operators cable box will have the necessary software or decryption software or a module that is attached or is in communication with the cable box receiver that allows the decryption of the incoming encrypted data packets, due to the fact the data packets and as well as the encryption key sent from the operators server will be encrypted.);

- computer code for processing the decrypted data packets and the unencrypted_data packets by the sink device(Col. 3, lines 5-9, the examiner notes that the cable box or the operators cable box will have the necessary software or decryption software or a module that is attached or is in communication with the cable box receiver that allows the decryption of the incoming encrypted data packets, due to the fact the data packets and also encryption key from the operators server will be encrypted.); and

- computer readable medium for storing the computer code (Col. 3, lines 5 – 9 & Col. 3, lines 47 – 50, the examiner notes that the customers receiver(i.e. cable box, which is portable) can be considered a computer program product. Based on the fact that a cable box has both a hardware and software components, without the hardware component or

software component, the other component will be unable to operate; the cable box contains the necessary software to retrieve TV programming (i.e. movies, sporting events etc.) from the operators server, which is a computer, which is able to communicate and or read the signals from the cable box, initiated by the customer or user commands, the receiver is also able to interpret the operators server commands.)

Claim #17. A method as recited in claim 1, further comprising:

- forming a second group of encrypted data packets by encrypting some of the number of data packets not already encrypted based upon a second set of encryption values(Col. 3, lines 47 –50, the examiner notes that if a customer requests a movie or other TV programming from the cable TV operator, a forming of the multimedia data packet content (i.e. movie) will occur at the service operator (i.e. the source), the data packets will be sent in groups in a consecutive order (i.e. first group of encrypted data packets, and second group of encrypted data packets etc.) and each group of data packets are encrypted with different keys in order to prevent a hacker from copying or obtaining the multimedia content, the use of different keys to encrypt the different segments of the various multimedia content is done so only a segment of a multimedia transmission is compromised instead of the entire multimedia content transmission.); and

- decrypting the second group of encrypted data packets using the second set of encryption values concurrently with the decrypting of the first set of encrypted data packets (Col. 3,

lines 47 –50, the examiner notes that once the data packets reach the sink device, the decryption module will decrypt the data packets that correspond with the encryption/decryption key received in the multimedia transmission.)

Claim #18. A method as recited in claim 17, wherein

- the first set of encryption values is different than the second set of encryption values (Col. 3, lines 47 –50, the examiner notes that if a customer requests a movie or other TV programming, a forming of the multimedia data packet content (i.e. movie) will occur at the service operator (i.e. the source) the data packets will be sent in groups in a consecutive order (i.e. first group of encrypted data packets, and second group of encrypted data packets etc.) and each group of data packets are encrypted with different keys in order to prevent a hacker from copying or obtaining the multimedia content as a whole, once only one of the groups of data packets are compromised. Also, if a customer orders another movie (i.e. multimedia content) this is also considered a second group of a forming of data packets and encryption values.

### *Claim Rejections - 35 USC § 103*

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim(s) 3 & 4, 14 & 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Huuhtanen (Publication # EP 0 674 441 A1) in view of Pasqualino (PGPUB # 2002/0163598) Huuhtanen discloses forming a first group of encrypted data packets by encrypting some of the data packets based upon a first set of encrypted/decrypted values, wherein the number of encrypted data packets in the first group of encrypted data packets is less than the number of data packets formed at the source device, Col. 3, lines 47-49)

Huuhtanen does not appear explicitly disclose Vsync, Hsync , CNTL3 which are all control or timing signals that can be used in, communicating data over a communications link and the encryption and decryption of data packets according to HDCP (encryption/decryption engine).

However, Pasqualino teaches Vsync, Hsync , CNTL3 which are all control or timing signals that can be used in, communicating data over a communications link and the encryption and decryption of data packets according to HDCP (encryption/decryption engine), Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3)

Huuhtanen and Pasqualino are analogous art because they are from the same field of endeavor of encrypting and decrypting of data sent over an unprotected communication link between a source and sink device.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Huuhtanen and Pasqualino before him or her, to modify the forming of a

plurality of data packets at the source and selecting a some of the data packets to scramble of Huuhtanen to include the control signals associated with the transmission of data packets of Pasqualino, because by selecting only some of the plurality of data packets to be encrypted and associating a specific control packet and encryption/decryption values will allow the receiver to identify the incoming data packets that are encrypted and unencrypted. This protocol will also make it very hard to obtain an illegal signal from the cable service operator, due to the fact that each successive grouping of data packet has different encryption/decryption values and control packet.

The suggestion/motivation for doing so would have been to prevent non-paying or non-subscribing customers from obtaining or pirating free service (Pasqualino: Paragraph: 0053) and preventing the pirating of all video and audio stream content or data packets being transferred from a source (TV operators equipment) to a sink (customers cable TV box) in a lossless digital domain. (Pasqualino: Paragraph: 49).

Therefore it would have been obvious to combine Huuhtanen and Pasqualino to obtain the invention as specified in the instant claims.

Claim(s) 5 &11 &16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Huuhtanen (Publication # EP 0 674 441 A1) in view of Pasqualino (Publication #2002/0163598 A1)

Huuhtanen teaches forming a second group of encrypted data packets by encrypting some of the data packets based upon a second set of encrypted/decrypted values, wherein the number of encrypted data packets in the second group of encrypted data packets is less than the number of data packets formed at the source device, Col. 3, lines 47-49).

Huuhtanen does not appear to teach Vsync, Hsync , CNTL3 which are all control or timing signals that can be used in, communicating data over a communications link and the encryption and decryption of data packets according to HDCP (encryption/decryption engine)

However, Pasqualino teaches Vsync, Hsync , CNTL3 which are all control or timing signals that can be used in, communicating data over a communications link and the encryption and decryption of data packets according to HDCP (encryption/decryption engine), Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3)

Huuhtanen and Pasqualino are analogous art because they are from the same field of endeavor of encrypting and decrypting of data sent over an unprotected communication link between a source and sink device.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Huuhtanen and Pasqualino before him or her, to modify the forming of a plurality of data packets at the source and selecting a some of the data packets to scramble of Huuhtanen to include the control signals (CNTL3) associated with the transmission of data

packets (i.e. identify which data packets are encrypted) of Pasqualino, because by selecting only some of the plurality of data packets to be encrypted and associating a specific control packet and encryption/decryption values will allow the receiver to identify the incoming data packets that are encrypted and unencrypted. This protocol will also make it very hard to obtain an illegal signal from the cable service operator, due to the fact that each successive grouping of data packet has different encryption/decryption values and control packet.

The suggestion/motivation for doing so would have been to prevent non-paying or non-subscribing customers from obtaining or pirating free service (Pasqualino: Paragraph: 0053) and preventing the pirating of all video and audio stream content or data packets being transferred from a source (TV operators equipment) to a sink (customers cable TV box) in a lossless digital domain. (Pasqualino: Paragraph: 49).

Therefore it would have been obvious to combine Huuhtanen and Pasqualino to obtain the invention as specified in the instant claims.

Claim(s) 19 is rejected under 35 U.S.C. 103(a) as being unpatentable Huuhtanen (Publication # EP 0 674 441 A1) over in view of Pasqualino: (Pgub # 2002/0163598 A1)

Huuhtanen teaches forming a second group of encrypted data packets by encrypting some of the data packets based upon a second set of encrypted/decrypted values, wherein the number of

encrypted data packets in the second group of encrypted data packets is less than the number of data packets formed at the source device, Col. 3, lines 47-49).

Huuhtanen does not appear to teach Vsync, Hsync , CNTL3 which are all control or timing signals that can be used in, communicating data over a communications link and the encryption and decryption of data packets according to HDCP (encryption/decryption engine)

However, Pasqualino teaches Vsync, Hsync , CNTL3 which are all control or timing signals that can be used in, communicating data over a communications link and the encryption and decryption of data packets according to HDCP (encryption/decryption engine), Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3)

Huuhtanen and Pasqualino are analogous art because they are from the same field of endeavor of encrypting and decrypting of data sent over an unprotected communication link between a source and sink device.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Huuhtanen and Pasqualino before him or her, to modify the forming of a plurality of data packets at the source and selecting a some of the data packets to scramble of Huuhtanen to include the control signals (CNTL3, VSYNC, HSYNC) associated with the transmission of data packets (i.e. identify which data packets are encrypted) of Pasqualino, because by selecting only some of the plurality of data packets to be encrypted and associating a

specific control packet and encryption/decryption values will allow the receiver to identify the incoming data packets that are encrypted and unencrypted. This protocol will also make it very hard to obtain an illegal signal from the cable service operator, due to the fact that each successive grouping of data packet has different encryption/decryption values and control packet.

The suggestion/motivation for doing so would have been to prevent non-paying or non-subscribing customers from obtaining or pirating free service (Pasqualino: Paragraph: 0053) and preventing the pirating of all video and audio stream content or data packets being transferred from a source (TV operators equipment) to a sink (customers cable TV box) in a lossless digital domain. (Pasqualino: Paragraph: 49).

Therefore it would have been obvious to combine Huuhtanen and Pasqualino to obtain the invention as specified in the instant claims.

## *Response to Arguments*

Applicant's arguments with respect to claim(s) 1, 6, 12 have been considered but are moot in view of the new ground(s) of rejection. The reference Huuhtanen (Publication # EP 0 674 441 A1) teaches (Col. 3, lines 47 – 49, that the a plurality of data packets are formed at the source (cable TV operator source) and only a select few (Col. 4, lines 14 – 18 ) of the data packets are encrypted and sent over the unsecured communications link to a sink device ,

(customers receiver box (i.e. set up top box)), which has a decryption means to decrypt the incoming encrypted data packets.)

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JOSEPH DEL SOLE
SUPERVISORY PATENT EXAMINER
6/19/07